Published and Copyright (c) 1999 - 2008
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1114 04/03/09

~ Conficker Peters Out! ~ People Are Talking! ~ CCAG 2009 in May!
~ IBM Taking Over Sun! ~ eBay Tests eBay Bucks! ~ Chinese Cyber Spies!
~ China Goes into Denial ~ Unpaid Bills & Laptops ~ Spammers Sentenced!

~ Spam Recovers from KO! ~ DSI To Arrive Sunday! ~ FBI Raids Core IP!

-* Bullying Bill Includes Posts *-
-* Online Crime Surging in Recession! *-
-* Court Won't Revive Virginia Anti-Spam Law! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

It's been another one of those long and tiring weeks. I don't even have the energy to rant about politics and the economy - probably thankfully! So, rather than put you through another week of lousy New England weather and the slow evolution of Spring, let's get right to this week's issue!

Until next time...

=~=~=~=

->A-ONE User Group Notes! - Meetings, Shows, and Info!
"""""""""""""""""""""""""

The CCAG 2009 Show Is Coming Soon!

Buy, sell, trade, play, and see classic video games, computers, peripherals, memorabilia, and more at the Classic Computing and Gaming Show (CCAG) on May 23, 2009 at the American Legion Hall--Clifton Post, 22001 Brookpark Rd, Fairview Park, OH from 12:00 PM - 8:00 PM. Vendors, clubs, and collectors will be displaying and selling their retrogaming and retrocomputing goods, from Pong and Atari to Nintendo, Apple and IBM to Commodore and everything in between with many set up for you to play with and explore. The cost for admission is $2.00 for adults and 1.00 for kids 12 and under. All paid admissions come with a FREE Special CCAG Edition Video Game Trader Guide, 3 FREE Chinese Auction Coupons to win some cool and valuable prizes, FREE Arcade and Tournament Play and so much more. We have 4000+ square feet of space. Help us fill it all up!

For more information please go to http://www.ccagshow.com/

=~=~=~=

PEOPLE ARE TALKING

compiled by Joe Mirando
joe@atarinews.org

Hidi ho friends and neighbors. Well, the meager handful of messages in the NewsGroup this week just isn't enough to put in a column, even when teamed up with the handful from last week. I guess about all I can do is hang on to them and hope for better luck next week.

I don't really want to talk about politics this week, but I think the economy might be a good topic.

Yeah, the economy sucks. End of conversation.

I know, that's not much in the way of insight, but it IS true. Right now it might seem that the "how" and "why" of it is less important than getting us out of it, but that only leads to it happening again because we didn't learn from it to begin with.

The economy is an interesting 'creature'. It evolves. It goes through stages and modifies itself (okay, not itself... WE... or SOME of we.. modify it). After the Great depression, we modified it so that banks couldn't collapse in the normal course of... well, banking.

Well, it took about 50 years, but the industry itself found a way around the safeguards like a child defeating a safety gate.

Through several iterations and re-inventions of itself, the banking industry evolved into something where the depositors' money wasn't their product, the interest and profit earned from the wise investment of capital was their product. The service provided to the institution itself, the depositors or the system itself was no longer their product.

Their product became their stock shares. The lending and borrowing of money just became an inconvenient intermediate step along the way. That's the same thing that happened to General Motors, in my opinion. They became more concerned at the top levels with making their stock offering look good and forgot about that pesky intermediate step... the American automobile.

So yes, we will fix the 'holes' in the system. And in time the system will find ways around it. Gone are the days when a savings account was a good idea. Banks don't pay enough interest to even keep up with inflation, and because of that, less people are saving with them. So the banks have even less incentive to give people incentive to save with them which, of course gives the banks less incentive to... well, you get the idea. Pretty soon, they may be charging US interest to have money in a savings account. So most banks spend their time making their balance sheets look good so that they can attract a larger bank to buy them.

Failing that, bundling mortgages and loans for sale as securities/derivatives is what they seem to feel is a good way to make a profit. Unfortunately, in order to make it work, you have to bundle a LOT of loans and mortgages. Some of them are going to be 'bad' loans. You can get 'insurance' to protect yourself and your blessed investors. Enter AIG.

So, if you don't have to worry about taking a loss, you can include anything you want in these "bundles". Most of 'em will probably work out

and, if they don’t, well, that’s what insurance is for, right?

But all that goes out the window as more and more of the stuff you bundled turns bad... mortgages that shouldn’t have been made on properties that people couldn’t afford at interest rates that would change for the worse. But that’s okay, but there’s always the insurance... until the ’insurance company’ can’t cover ITS bets. And that’s what insurance is... a bet. When you buy a life insurance policy, you’re basically betting that you’re going to die before the policy, and the insurance company is betting that you won’t.

So that, dear friends, in a nutshell, is my take on why we need to fix things... and why the industry will again find ways to be corporations instead of institutions.

We will, of course, come out of this. But it will not be easy and it will not be cheap. And if we sit back and figure that we’ve fixed the problem for good, it will happen again in a slightly different fashion.

Wish I has something more hopeful and uplifting for you, but that’s the way I see it.

Hopefully, there will be enough traffic in the NewsGroup next week to have something cool to talk about. Until then keep your ears open so that you’ll hear what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week’s Gaming Section - DSI To Arrive on Sunday!
Sony Cuts PS2 Price!
New Xbox in the Works?
And much more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!

Sony Cuts Price of PlayStation 2, Not PS3

Sony Corp said it cut the price of its older video game console, the PlayStation 2, by 23 percent to $99.99, in an attempt to woo budget-minded families.

The price cut, effective April 1, could sustain the life of the PS2, which has sold more than 136 million units since its debut in 2000, making it the world’s popular gaming system, Sony said on Tuesday.

The news follows - and momentarily puts to rest - rumors on video gaming websites and blogs that Sony might cut the price of the PlayStation 3, its more powerful console. The PS3's least expensive model sells for about $400.

Sony said that the sub-$100 price will draw in a new wave of customers ranging from lower-income families to gamers who may have passed on pricier new systems. In addition, it may give incentive to retailers to keep PS2 on store shelves.

Sony dominated the global video game industry for a decade starting in the mid-1990s, but sales of the PS3 have lagged behind those of Nintendo Co Ltd's Wii console and Microsoft Corp's Xbox 360.

Microsoft's sales got a boost in September after it cut prices on some Xbox 360 models by about $50. The company said it sold 28 million units worldwide in 2008, outpacing the PS3 by over 8 million units.

While still considered pricey, video game consoles continue to post robust sales even as consumers think twice about discretionary spending amid the recession.

Most generations of new console are retired after about a decade, when developers move on to focus on more advance machines. Not true for the PS2, which sold some 2.5 million units in the U.S. alone last year, and remains profitable for Sony even at the new price level, according to John Koller Hardware marketing director at Sony Computer Entertainment.

He said that developers are making plans for the system as much as 3 years out, with up to 80 new games are in the works for the system this year and another 70-80 due in 2010.

"There is no reason to slow down any of the momentum on the console now," he said. "There is no retirement tour or clock on the wall. As long as it continues to sell at the viable levels that it is, we are going to sell and market the platform."

Asked to comment on any plans that Sony has for cutting the price of the PS3, Koller said: "We feel good about where PlayStation 3 is. We continue to monitor the business."

Despite the resilience of the PS2, so-called "next generation" consoles are still the industry's first priority. The PS3, Xbox 360 and Wii are often a centerpiece in the home that can deliver many hours of disc-based, online and collaborative gaming. All but the Wii play DVDs and can stream Internet movies.

Citing that reason, Microsoft said Sony's price cut does not address the future of the video game industry.

"We believe, however, that the future lies in the growth of current generation consoles and Xbox 360, as the fastest growing games console last year...will continue to drive the market," said Microsoft's Chris Lewis, who is Regional Vice President of Interactive Entertainment Business in Europe.

Nintendo Rolls Out DSi to U.S. on Sunday

Nintendo is rolling out the next generation of its popular handheld gaming console in the United States on Sunday, pitching the product as more of an all-purpose social and entertainment device.

Aside from game-playing functions, the dual-screen DSi features two cameras, a microphone and a host of tools that will allow users to create content and share with others.

The DSi will retail for $170 apiece and began selling in Europe on Friday. The third generation in the DS franchise, the DSi was launched in Japan last November and has so far sold 2 million units.

"This thing is to the digital camera what the iPod was to the MP3 player," said Wedbush Morgan analyst Michael Pachter. "You take the same form factor and you just add something to it and suddenly you're going to have a lot of people carrying it."

Nintendo's second-generation DS handheld, the DS Lite, will continue to sell for $130. Nintendo has shipped more than 100 million DS units overall since the franchise launched in late 2004.

Cammie Dunaway, executive vice president of sales and marketing for Nintendo America, said the DSi seeks to make the traditional gaming experience more personalized.

"How do you get a Nintendo game device in every briefcase and backpack and pocketbook? We realized that what you need to make that happen is a device that is highly customizable... Natural tools for customization are things like photos," she said.

Pachter said he expects the device to appeal to teens and tweens.

"They're going to turn a one DS household into a two DS household. You will hand it down to your little brother when you get your DSi."

Nintendo's DS line competes directly with Sony's PSP handheld device and increasingly faces competition from Apple's iPhone, which is emerging as a serious video game platform, and iPod touch devices.

The PSP has sold more than 50 million units, while the iPhone and iPod Touch have combined to sell more than 30 million.

Nintendo is also launching a new online store where DSi users can download new games and applications via the device's WiFi connection. The store will also offer a DSi Internet browser for download, based on the Opera browser.

Nintendo has been credited with helping expand the traditional demographic profile of the gaming industry. The company's Wii console has been a hit with consumers, attracting adults and females who are more interested in casual and social games.

The Wii, Nintendo's console platform, has sold more than 50 million units worldwide since its release in 2006.

Yes, Microsoft's Working on an Xbox Next. Surprised?

Sometimes it’s what a company say it’s *not* doing that grabs your head and twists it around. Case in point, Blizzard veep of game design Rob Pardo is flatly denying rumors the company’s been rapping with Microsoft about a hypothetical Xbox 360 successor (unimaginatively dubbed ’Xbox 720’ by the mathematically literalist media).

Pardo reportedly told folks at GDC that Blizzard was talking with Microsoft about its next-gen games console. And then he told GameSpot he wasn’t.

It’s no secret high level execs yak about this stuff behind hermetically sealed walls and chambers, probably carrying around microscopic explosives that could blow open their carotid arteries if they squeal. Occasionally something leaks anyway (or appears to) then bangs around the blogosphere with exaggerated gravitas.

With the Xbox 360 over three years old, it’s as likely as not that Microsoft’s already broached the subject of its Xbox 360 followup act (in one form or another) with whoever it’s dubbed worthy. But that’s about as prescient on my part as suggesting Toyota’s presently rendering concept sketches of its 2012-2013 midsize lineup, i.e. "it’s the common sense, stupid."

And besides...

Who cares?

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Online Crime Surging in Recession

Fraud on the Internet reported to U.S. authorities increased by 33 percent last year, rising for the first time in three years, and is surging this year as the recession deepens, federal authorities said on Monday.

Internet fraud losses reported in the United States reached a record high $264.6 million in 2008, according to a report released on Monday from the Internet Fraud Complaint Center, run by the FBI and the National White Collar Crime Center.

Online scams originating from across the globe - mostly from the United States, Canada, Britain, Nigeria and China - are gathering steam this year with a nearly 50 percent increase in complaints reported to U.S. authorities in March alone.

"2009 is shaping up to be a very busy year in terms of cyber-crime," the report’s author, John Kane, told reporters in a telephone briefing.

Last year’s losses compared with $239.1 million in 2007 and dwarfs the $18 million of losses of 2001.

The most common complaint of 2008 was non-delivery of promised merchandise, followed by auction fraud, credit card fraud and investment scams, according to the report.

Of 275,284 complaints received by the center in 2008, some 72,940 were referred to U.S. law enforcement agencies for prosecution. Those referrals spiked this year with 40,000 in the first quarter alone, said Kane.

"It is our belief that these numbers, both the complaints filed and the dollars, represent just a small tip of the iceberg," said Kane, managing director of the National White Collar Crime Center in Richmond, Virginia.

"Our own research suggests that as few as 15 percent of cases of cyber-fraud are being reported to crime control agencies," he said.

Scammers in the United States comprised 66 percent of complaints referred to authorities, followed by Britain at 11 percent, Nigeria 7.5 percent, Canada 3 percent and China 1.6 percent. Within the United States, the bulk originated in California (16 percent), followed by New York and Florida.

Fraudulent sales on online auction sites like eBay Inc and classified sites like craigslist.com contributed to a 32 percent rise in the hottest area of online fraud - non-delivery of promised merchandise, the report said.

That area alone made up about 33 percent of all complaints serious enough to be referred to law enforcement.

Other important areas included investment scams such as mini-versions of the $65 billion Ponzi scheme committed by New York financier Bernard Madoff in which money from new investors is used to pay existing investors.

About 74 percent of the scams were through e-mail messages last year, especially spam, while about 29 percent used websites. But criminals were increasingly tapping new technologies such as social networking sites and instant messenger services, said Kane.

The report highlights one new "significant’ identity-theft scam involving e-mail messages that give the appearance of originating from the FBI but seek bank account information to help in investigations of money being transferred to Nigeria. Recipients of the e-mails are told they could be richly rewarded by cooperating.

The report said almost 80 percent of known perpetrators of online scams are male. Of those bringing complaints, nearly half are between the ages of 30 and 50. The median dollar loss was $931 per complaint, although the median losses for check fraud reached $3,000 and that for investment scams was $2,000.

Cyber Spies Break into Government Computers

A cyber spy network based mainly in China hacked into classified documents from government and private organizations in 103 countries, including the computers of the Dalai Lama and Tibetan exiles, Canadian researchers said Saturday.

The work of the Information Warfare Monitor initially focused on allegations of Chinese cyber espionage against the Tibetan community in exile, and eventually led to a much wider network of compromised machines, the Internet-based research group said.

"We uncovered real-time evidence of malware that had penetrated Tibetan computer systems, extracting sensitive documents from the private office of the Dalai Lama," investigator Greg Walton said.

The research group said that while it’s analysis points to China as the main source of the network, it has not conclusively been able to detect the identity or motivation of the hackers.

Calls to China’s Foreign Ministry and Industry and Information Ministry rang unanswered Sunday. The Chinese Embassy in Toronto did not immediately return calls for comment Saturday.

Students For a Free Tibet activist Bhutila Karpoche said her organization’s computers have been hacked into numerous times over the past four or five years, and particularly in the past year. She said she often gets e-mails that contain viruses that crash the group’s computers.

The IWM is composed of researchers from Ottawa-based think tank SecDev Group and the University of Toronto’s Munk Centre for International Studies. The group’s initial findings led to a 10-month investigation summarized in the report to be released online Sunday.

The researchers detected a cyber espionage network involving over 1,295 compromised computers from the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan. They also discovered hacked systems in the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan.

Once the hackers infiltrated the systems, they gained control using malware - software they install on the compromised computers - and sent and received data from them, the researchers said.

Two researchers at Cambridge University in Britain who worked on the part of the investigation related to the Tibetans are also releasing their own report Sunday.

In an online abstract for "The Snooping Dragon: Social Malware Surveillance of the Tibetan Movement," Shishir Nagaraja and Ross Anderson write that while malware attacks are not new, these attacks should be noted for their ability to collect "actionable intelligence for use by the police and security services of a repressive state, with potentially fatal consequences for those exposed."

They say prevention against such attacks will be difficult since traditional defense against social malware in government agencies involves expensive and intrusive measures that range from mandatory access controls to tedious operational security procedures.

The Dalai Lama fled over the Himalaya mountains into exile 50 years ago

when China quashed an uprising in Tibet, placing it under its direct rule for the first time. The spiritual leader and the Tibetan government in exile are based in Dharmsala, India.

Court Won’t Revive Virginia Anti-Spam Law

The Supreme Court will not consider reinstating Virginia’s anti-spam law, among the nation’s toughest in banning unsolicited e-mails.

The court on Monday said it will leave in place a ruling by the Virginia Supreme Court that the law was unconstitutional because it prohibited political, religious and other messages in addition to commercial solicitations.

Virginia was the only state to ban noncommerical spam e-mail.

The decision also cements the reversal of the conviction of Jeremy Jaynes, who once was considered one of the world’s most prolific spammers. Jaynes bombarded Internet users with millions of pieces of spam, all of it commercial.

In 2004, Jaynes became the first person in the U.S. to be convicted of a felony for sending unsolicited bulk e-mail. He was sentenced to nine years but is currently serving time in federal prison on an unrelated conviction for securities fraud.

The case is Virginia v. Jaynes, 08-765.

Three Spammers Sentenced in US for Advance Fee Fraud

Two Nigerians and a Frenchman were sentenced to prison Thursday for swindling people out of more than US$1.2 million in a massive e-mail scam, the U.S. Department of Justice said.

Nnamdi Chizuba Anisiobi, 31, of Nigeria was sentenced to 87 months in prison, while Anthony Friday Ehis, 34, of France and Kesandu Egwuonwu, 35, of Nigeria were sentenced to 57 months. They were sentenced in U.S. District Court for the Eastern District of New York.

After being arrested in Amsterdam in February 2006, all three were extradited to the U.S. The DOJ said all three pleaded guilty to one count of conspiracy, eight counts of wire fraud and one count of mail fraud. Mail and wire fraud carry maximum possible sentences of 20 years in prison, while conspiracy has a maximum penalty of five years.

The three men executed so-called advance fee frauds. Victims were told their help was needed distributing money for charity. In exchange, victims were promised they would get a commission that would go to the charity of their choice, the DOJ said.

The victims were told they first needed to wire-transfer money for various fees. In some cases, victims were sent counterfeit checks in order to the cover the fees, which bounced even though victims already sent money, DOJ said.

In one variation of the scam, people were sent an e-mail that purported to be from someone suffering from terminal throat cancer who needed help distributing $55 million in charity money. The victims were told they would get a 20 percent commission that would go to a charity of their choice for their trouble.

To make the ruse seem more legitimate, the scammers sent photos of the supposed throat cancer victim, along with other fraudulent documents that ostensibly confirmed the $55 million, the DOJ said.

Advance fee frauds have become so prevalent that law enforcement and private companies have undertaken new steps to stop the scams.

In October 2008, the Advance Fee Fraud Coalition was created to educate the public about the frauds as well as foster closer cooperation between police and industry. Members of the coalition include Microsoft, Yahoo, the money-transfer agency Western Union and the African Development Bank.

Microsoft and Yahoo are particularly concerned about advance fee frauds since the criminals often use their free e-mail accounts to send bogus pitches. The fraudsters have also hijacked those brands, sending e-mails that purport to be a lottery sponsored by Microsoft or Yahoo.

Ultrascan Advanced Global Investigations in the Netherlands, which has a special department dedicated to investigating advance fee frauds, estimates that $4.3 billion was lost to that type of scam in 2007.

The Eight Things You Need to Know About ’Conficker’

On Wednesday, April 1, the latest variant of the Conficker (also known as Downadup and Kido) work will download new instructions. The sophistication of this worm and its botnet have many concerned, although the amount of legitimate concern is a matter of debate.

If you’re concerned, then here are the eight most important things to know about Conficker, updated on Monday morning:

1. Researchers have discovered what they’re calling a signature for Conficker, and developed a scanner based upon the technology.

2. The overwhelming majority of systems infected with Conficker were infected through a vulnerability in the Windows RPC facilities. This vulnerability was patched in October. If you installed that patch before Conficker came out (late December ’08) then you were protected and still are. If you haven’t installed the update then it’s essential that you do so. Windows Vista is technically vulnerable in this way, but the exploit is almost impossible to execute on it. Conficker is basically an XP problem.

3. Conficker can also spread through network shares, including those that have weak passwords; the worm executes a "dictionary attack" in which a list of common passwords (think "password", "asdf", etc) are used to gain access to the share. So if you find new executables on such drives they may be infected. Treat them as you would a program that got e-mailed to you unsolicited, and we hope that means you’ll avoid it and report it to a network admin if you have one. A good anti-malware

program will detect it at this stage.

4. It follows from this advice that you are also better off by using complex and unobvious passwords, especially those that use both numerals and letters and especially if they include punctuation.

5. Conficker can also spread by putting itself on removable drives like USB drives. When it does so it sets the Autorun on those drives to run itself. So if you insert such a drive you could, at the least, get a standard Windows Autoplay menu offering Conficker among its options. Sometimes it will disguise itself as the Windows option for opening Windows Explorer for the inserted drive. Once again, a good anti-malware program will detect it at this stage.

6. Anti-malware software isn't perfect but it has a very high rate of success. Conficker is about as high-profile as malware gets; all the companies have it and understand it well, and so if you have anti-virus software and keep it up to date it's hard for you to get attacked.

7. Conficker can interfere with the ability of Windows and anti-malware programs to update themselves. Ensure that they are doing so by checking the last update date/time of your anti-malware software and by checking Windows Update manually. Leave no critical updates uninstalled.

8. Free Conficker/Downadup Cleaning Tools:

* McAfee Stinger
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=11vjjjuh2/*http://vil.nai.com/vil/conficker_stinger/Stinger_Coficker.exe>

* ESet EConfickerRemover
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=11olhobs1/*http://download.eset.com/special/EConfickerRemover.exe>

* Symantec W32.Downadup Removal Tool
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=12q8n58a3/*http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99>

* F-Secure F-Downadup, FSMRT, more tools
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=11s7cep7b/*http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml>

* BitDefender single PC and network removal tools
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=10pfi2jpf/*http://www.bdtools.net/>

* Kaspersky KKiller
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=121il3tcd/*http://data2.kaspersky-labs.com:8080/special/KKiller_v3.4.1.zip>

* Trend Micro
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=12pj6npch/*http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-WORM_DOWNAD.zip>

  If you use one of these tools to remove Conficker immediately

install the MS08-067 patch afterwards.

* BitDefender
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=12bqhb4qj/*http://www.bitdefender.com/VIRUS-1000462-en--Win32.Worm.Downadup.Gen.html>

* Symantec
  <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/238653/31485681/SIG=12q8n58a3/*http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99>

Don’t Fret About Conficker: Here’s What To Do

The Conficker worm, a nasty computer infection that has poisoned millions of PCs, will start ramping up its efforts Wednesday to use those machines for cybercrimes. It’s unclear whether everyday PC users will even notice, but this is as good an excuse as any to make sure your computer is clean.

There are some easy ways to figure out whether a computer has the Conficker worm, and free tools available for getting rid of it.

One scary thing about Conficker is that it spreads without human involvement, moving from PC to PC by exploiting a security hole in Microsoft Corp.’s Windows operating system. The hole was fixed in October, but if your computer doesn’t get automatic updates from Microsoft, you could be vulnerable.

Lots of computer worms disable antivirus software outright, which can be a tip-off that something is wrong. But Conficker doesn’t do that. Instead, Conficker blocks infected PCs from accessing the antivirus vendors’ and Microsoft’s Web sites, so victims won’t get automatic updates and can’t download the Conficker removal tools that those companies have developed.

So see what Web sites you can visit. If you can navigate the Internet freely except for sites owned by Microsoft or antivirus vendors such as Symantec Corp., McAfee Inc. or F-Secure Corp., your PC might have Conficker or a similar bug.

Fixing the problem gets a little trickier.

The best remedy is to have a friend, whose computer is not infected, download a removal tool from Microsoft or one of the antivirus vendors. Then that person should e-mail the tool to you.

A list of the free Conficker removal programs is available on the Web site of the Conficker Working Group, an alliance of companies fighting the worm. The removal programs will take care of themselves, for the most part, scanning your system and purging the worm.

One thing to note: Conficker blocks infected machines from running removal tools with "Conficker" in the name. So users might have to change the name of the file (one you’ve saved the tool to your desktop, right-click on it and select "rename") before running it. The program’s instructions will let you know if you need to do this. Many antivirus vendors have already changed the names in their removal tools, in some cases calling the file a misspelled variant of "Conficker", to trick

the worm into letting the program run.

Businesses have a bigger challenge, because Conficker has yet another method for evading detection. Once the worm is inside a machine, it applies its own version of the Microsoft patch that fixes the vulnerability Conficker exploited in the first place. So a business running a standard network scan, looking for unpatched machines, might come up empty-handed, even though some computers on the network are infected.

The scans need to take a deeper dive into the machines on the network, something an antivirus vendor's service should enable. For government agencies, contractors and operators of critical infrastructure, the Department of Homeland Security also has released a network-detection tool for Conficker.

Conficker Worm Reaches Go Time, to No Effect

The Conficker Internet worm's feared April Fools' Day throwdown for control of millions of infected PCs stirred lots of panic but came and went with a whimper.

Security experts say some Conficker-infected computers - those poisoned with the latest version of the worm - started "phoning home" for instructions more aggressively Wednesday, trying 50,000 Internet addresses instead of 250. However, security companies monitoring the worm remained successful at blocking the communications.

"We didn't see anything that wasn't expected," said Paul Ferguson, a security researcher at antivirus software maker Trend Micro Inc. "I'm glad April 1 happened to be a nonevent. People got a little too caught up in the hype on that. (The infected computers) didn't go into attack mode, planes didn't fall out of the sky or anything like that."

The worm can take control of unsuspecting PCs running Microsoft's Windows operating system. Tied together into a "botnet," these PCs can be directed to send spam, carry out identity-theft scams and bring down Web sites by flooding them with traffic.

That's why the April 1 change in Conficker's programming was a small twist - and not the end of the story. The network of Conficker-infected machines could still spring to life and be used for nefarious deeds.

One scary element is that Conficker's authors have given the infected PCs peer-to-peer abilities, which allows them to update each other and share malicious commands through encrypted channels. That ability means the computers don't have to contact a Web site at all, and the communications are protected.

And the criminals behind Conficker are likely taking their time.

"The people who are pulling the strings on this are very slow and determined and measured in making modifications to this botnet," Ferguson said. "Basically, they're building a layer of survivability."

Conficker spreads without human involvement, moving from PC to PC by exploiting a security hole in Microsoft Corp.'s Windows operating

system. In October, Microsoft issued a software update, called a "patch," to protect PCs from the vulnerability, but not everyone applied the patch.

In one telltale sign of an infected machine, Conficker blocks Microsoft's site as well as those of most antivirus companies. Computer owners can work around that obstacle by having someone else e-mail them a Conficker removal tool.

Security researchers don't have a firm estimate of the number of Conficker-infected machines. There appear to be at least 3 million infected PCs, and possibly as many as 12 million, but tallies vary because some machines may have been counted multiple times, and the number fluctuates as PCs are scrubbed clean of the infection while other machines are compromised.

IBM in Final Stages of Deal Talks with Sun

IBM Corp. and rival Sun Microsystems Inc. are in the final stages of negotiations over IBM's takeover of Sun. A deal could be announced within days.

Haggling over price is one reason the acquisition hasn't happened yet.

People briefed on the negotiations told The Associated Press that the last specifics of the deal are being worked out. These people spoke on condition of anonymity because they were not authorized to discuss the situation.

The New York Times and The Wall Street Journal reported on their Web sites Thursday that IBM will likely pay between $9 and $10 per share for Sun. Earlier discussions involved a price of about $10 to $11 per share.

A deal would shake up the corporate computing landscape and likely draw antitrust scrutiny.

Unpaid Bills? Good Luck Starting Future Laptops

As wireless carriers begin to subsidize computers that come with wireless Internet access, they're faced with a quandary: What do they do if the buyer stops paying his bills?

The company can cut off the computer's wireless access, but the carrier would still be out a couple of hundred dollars. The buyer would be left with a computer that's fully usable except for cellular broadband.

LM Ericsson AB, the Swedish company that makes many of the modems that go into laptops, announced Tuesday that its new modem will deal with this issue by including a feature that's virtually a wireless repo man. If the carrier has the stomach to do so, it can send a signal that completely disables the computer, making it impossible to turn on.

"We call it a 'kill pill,'" said Mats Norin, Ericsson's vice president of mobile broadband modules.

The module will work on AT&T Inc.’s U.S. third-generation network, and on many other 3G networks overseas.

AT&T late last year started subsidizing small laptops known as "netbooks," which normally cost about $400, so that RadioShack Corp. can sell them for $100. The buyer commits to paying $60 per month for two years for AT&T’s wireless broadband access. Such offers have become very common in Europe.

It’s unlikely that carriers would resort to wielding the "kill pill." But the technology, developed with Intel Corp., has other uses. For instance, a company could secure its data by locking down stolen laptops wirelessly. Lenovo Group Ltd. has said it will build this sort of feature into its laptops.

The new Ericsson modem can also stay active while a computer is off, listening for wireless messages. That means it could wake up and alert the user when it receives an important e-mail, or if someone is calling with a conferencing application like Skype.

Laptop makers that use Ericsson modules include LG Electronics Inc., Dell Inc., Toshiba Corp. and Lenovo.

W. Virginia Bullying Bill To Include Online Posts

An attempt to extend a West Virginia anti-harassment law to the Internet may have some long-reaching consequences.

Sen. Mike Green of Raleigh County sponsored the bill last week. The measure would make it a crime to send harassing or abusive e-mails or other computer-based communications.

But the Senate Judiciary Committee amended the bill to include statements posted on Web pages or online forums.

Such statements must be untrue and designed to encourage others to spread the falsehood, or ridicule the person they target.

Civil liberties advocates question whether that goes too far.

The bill would make such statements a misdemeanor, punishable by a fine of up to $500, up to six months in jail, or both. Repeat offenders would see those penalties double.

FBI Raids Dallas Internet Service Provider Core IP

U.S. Federal Bureau of Investigation agents have raided a Dallas ISP, knocking the company and almost 50 of its clients offline.

The early morning Thursday raid closed down the operations of Core IP Networks, which operated out of two floors of a Telx collocation facility at 2323 Bryan Street in Dallas. The raid had to do with the activities of a former customer, according to Matthew Simpson, Core IP’s CEO. "The FBI is investigating a company that has purchased services

from Core IP in the past," he wrote in a note posted to a Google Sites page. "This company does not even collocate with us anywhere, much less 2323 Bryan Street Datacenter."

He did not name the company that is allegedly at the center of the FBI investigation.

FBI spokesman Mark White confirmed that agents had executed a search warrant at the 2323 Bryan Street address on Thursday, but declined to comment further on the matter.

"Currently nearly 50 businesses are completely without access to their email and data," Simpson wrote. "Citizen access to Emergency 911 services are being affected, as Core IP’s primary client base consists of telephone companies. "

Simpson said that his company was not involved in any kind of illegal activity. He could not be reached immediately for comment.

It is unusual for the FBI to shut down an entire hosting provider because of the activity of a single customer.

Spam Recovers From a Knockout Blow

The Internet is now officially as bad as ever, at least as far as spam goes.

Google reported Tuesday that in the second half of March, spam returned to the levels last seen just prior to the November 2008 takedown of McColo. McColo was a hosting service based in San Jose, California, that was notorious for providing so-called "bulletproof" services to cybercriminals, who wanted to keep their servers running no matter what.

When McColo was knocked offline, it had a serious effect on the world’s junk e-mail. Spam levels dropped by half the instant the company’s upstream Internet service providers - Global Crossing and Hurricane Electric - refused to service the ISP, effectively unplugging McColo from the Internet.

"Spammers have clearly rallied following the McColo takedown and overall spam volume growth during Q1 2009 was the strongest it’s been since early 2008, increasing an average of 1.2 percent per day," wrote Google spokeswoman Amanda Kleha in a blog posting.

In the first quarter of last year, spam grew at 1 percent per day, which was a record at the time.

Data on another spam measurement site, Spamcop, also shows that spam has bounced back.

Spammers may be getting smarter, too, Kleha said. They seem to be building more robust botnets to send out their unwanted mail and also appear to be taking steps to avoid making their ISPs the kind of obvious target that McColo was.

"They have been building new botnets, like Conficker - which is undoubtedly designed to be difficult to take down," said Richard Cox,

CIO of antispam organization Spamhaus, in an e-mail interview. He agreed with Google's conclusion that spam had now returned to pre-McColo levels.

"Spammers continue to prove their resilience," Kleha said. "They're clearly here to stay."

China Denies Cyber Spy Network Charges

China on Tuesday denied suggestions it could be involved in a cyberespionage ring that attacked computers worldwide from servers mostly based in the country.

GhostNet, a network that affected 1,295 computers in more than 100 countries through malware and social engineering, was described in a study last weekend by the SecDev Group's Information Warfare Monitor and the Munk Center for International Studies at the University of Toronto.

"Some people in foreign countries are keen to make up rumors about so-called Chinese Internet spies," foreign ministry spokesman Qin Gang said at a briefing Tuesday. "Their statements are entirely fabricated."

China opposes hacking and other attacks on computer networks, Qin said.

Attackers used GhostNet to steal documents from targets including international institutions and foreign ministries of other countries, according to the report. The attackers gained full access to affected computers, including control of attached microphones and Web cams that could have been used to monitor nearby activity.

The report drew attention to cybercrime in China at a time when observers say it is growing. GhostNet's highly targeted attacks against foreign government networks are unique, but its scale is tiny and its malware code outdated compared to other recent attacks, analysts say.

A simple online search can reveal the source code for GhostNet's unsophisticated malicious software, said Zhao Wei, CEO of Knownsec, a Beijing security firm. Much more advanced - and more common in China - are mass attacks with "zero days," or previously unknown software bugs, Zhao said.

Sophisticated attacks can hit millions of computers. Researchers at Zhao's firm found 4 million computers infected in a single day during one recent attack.

China had 298 million Internet users at the end of last year, the most in any country, according to the country's domain registry center.

Bank accounts and online game passwords are popular targets for attackers in China. Items like armor and weapons stolen from game accounts are often sold back to other players for real-world cash.

The attackers can make themselves hard to catch by stealing small amounts from many different people, Zhao said. An attacker might, for example, break into a huge number of bank accounts but steal just 10 yuan (US$1.47) from each, an amount victims are unlikely to report. That makes collecting evidence difficult for police, as does the need for cooperation across districts if the attacker and victims are in

different places, Zhao said.

China passed its first regulations protecting the public from cyber data theft last month. The revisions to the country's criminal law ban digital theft of information from any computer, lowering the bar from old rules that banned intrusions into government-supported networks. The new law also prohibits designing programs to help attackers invade or gain control over other computers.

The law's protection from data theft extends to overseas computers like those attacked by GhostNet, said Pi Yong, a law professor at Wuhan University.

But implementing the law could be difficult even in purely domestic cases. Chinese courts in remote areas may be unsure how to handle electronic evidence, Pi said.

China also remains a convenient routing point for attackers from other countries, who can hide their location by using a Chinese IP (Internet Protocol) address.

Registering a Chinese domain is cheap and hassle-free, giving attackers an easy way to spread malware, said Konstantin Sapronov, head of the Kaspersky virus lab in China.

Blocked domains are easily replaced, he said.

"If it will be blocked, it doesn't matter. You can use another, and you can buy a lot of these," he said.

EBay To Test eBay Bucks Shopping Rewards Program

Shopping on eBay just got a bit more rewarding, at least for some users of the online auction site.

On Wednesday, eBay Inc. launched a "beta" test version of eBay Bucks, a program that lets participants earn a 2 percent reward on certain items they buy through the site and pay for using eBay's online payment service, PayPal. Rewards come quarterly as gift certificates, which can be used to buy other items through eBay within 30 days.

Unlike many other "beta" tests, this one is open by invitation only; eBay is randomly selecting buyers to enroll. Kurt Apen, head of eBay's loyalty marketing team, said the company will likely expand the program to everyone over the next several months.

The arrival of eBay Bucks marks the company's latest customer-retention move; something the company is focusing on as works to improve its online marketplace, at a time when consumers also have cut back on spending because of the dismal economy.

Other efforts eBay has undertaken include distributing coupons to users and offering discounts on referrals from Microsoft Corp.'s Live Search site.

Program participants will be able to earn up to $200 in eBay Bucks per item purchased on eBay and up to $500 per quarter. Because the reward rate is 2 percent, a $100 cell phone would earn $2 eBay Bucks,

translating to $2 in gift certificates at the end of the quarter.

Apen said eBay Bucks users will be able to collect rewards on most types of items sold on the site, but real estate and many items sold through eBay Motors will be ineligible.

EBay, based in San Jose, Calif., initially tested eBay Bucks as a smaller pilot program last year. Changes since then include making it easier for users to redeem their rewards and allowing them to spread them out over various transactions.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.